

EXPRESS MAIL Mailing Label No.: EL 394672045

ATTORNEY DOCKET NUMBER D/99748

5

**METHOD FOR VERIFYING CHRONOLOGICAL INTEGRITY OF AN
ELECTRONIC TIME STAMP**

10

This invention relates to the field of electronic document verification, and more particularly, to those methods of verifying the date and time of existence of electronic documents or files.

15

BACKGROUND OF THE INVENTION

20

In the arts organizations interested in protecting intellectual property or investigatory bodies, e.g. local and state police, FBI, private investigators, and the like, it is important to be able to verify ownership and time/date of creation of electronic papers and other electronic recordations thereby legally establishing what has happened, when something happened, and by whom. Since electronic media is alterable, establishing the accuracy of ownership and the date/time of creation can be difficult because computer system clocks can be set to inaccurate dates and/or times and electronic documents or files can be readily altered.

25

Much work has been done to date in the electronic document security and verification area in regards to the "what" and "by whom" (called non-repudiation) but typically time is not included in electronic non-repudiation because it is easy to set and change on computers. To overcome this, time of creation of electronic documents is established by other means such as sequencing of events. Emails are a good example of this. The order of emails sent and received can help investigators narrow down the time and date of creation by their order in the sequence. But, for other documents or files this sequencing for time and date of creation is not viable and, as the world quickly

progresses to an electronic "paperless" environment, solid techniques for establishing originality and time and date of origin are increasingly needed.

In order to secure passwords, system executables and high value data secure hash algorithms often are used to produce a "signature" that can later be
5 verified as originating from the owner. To secure data transmission integrity, several steps are typically employed. For instance, files are frequently combined into a "folder" or some other archive format and a data signature is generated of the archive file. Afterwards, the original archived file and its signature is placed in another archive file which is then encrypted with a private key. The use of a
10 certification authority or certificate authority can be additionally employed to ensure integrity of originality. For example, to support digital signatures, a trusted third party verifies the identity of that person or entity and then issues a digital certificate to the user that they sign digitally. The receiving person then verifies the digital signature as coming from a certified party.

15 There are cryptographic two signature algorithms in popular use, MD5 by RSA Data Security Inc and SHA1 by National Institute of Standards and Technology. Snefru was a signature algorithm developed by Xerox Corp, but is not used extensively. MD5 is the most common, but is also regarded as being likely to be compromised in the not too distant future. SHA1 was basically
20 designed as an open standard signature algorithm, but some trust the cryptographic strength behind it less than MD5 because of the general reputation of RSA.

At this point all of the focus on compromise of signature algorithms has been on the prevention replacement of an existing file with a substitute file with
25 the same signature. What will also be needed is to prevent the creation of a file with the same signature which can be associated with a previously generated time. Associating a signature with a file, its file size, and potentially with the signature of an encrypted transform of the file, and the signature of the encryption key is what this invention will use to prevent this type of forgery

In cryptography, there are various techniques of enhancing the "cryptographic" strength of a solution. Such techniques often involve the use of multiple encryptions or the use of encryptions where keys are of limited use (e.g. session keys). In mathematics there is a whole field of study in error correcting 5 codes. Applications in the computer field include parity bits. But error correcting codes extend to where errors can be both detected and corrected. For recoverability of a reliable time of existence, and the attributes of the files associated with the time, error detection and correction will be employed. Use of 10 error correcting codes in itself is a mathematical transformation of the electronic data. This invention will utilize error correcting codes to increase integrity, but also to increase cryptographic strength.

What is needed in the art and what is provided by this invention, is a method for securing the integrity of the time of existence of documents or files in preparation archiving such that the files' origin and authenticity can be 15 subsequently verified.

SUMMARY OF THE INVENTION

What is presented is a novel method of securing the chronological 20 integrity of files prior to archiving such that the files' origin and authenticity can be subsequently and readily verified. The method of the present invention involves the steps wherein the client first generates or otherwise acquires a Public and a Private Key pair. Preferably, the key pair is associated with an organization/corporate unit, or individual. If the key pair is reserved for archiving 25 then the risk of exposure and compromising is decreased. Commercial or private key infrastructures can be leveraged in this acquisition, but are not required. The client then generates a list of files to be archived along with the files' respective file sizes and cryptographic signatures.

The files data are then encrypted utilizing the client's Public Key. The 30 client transmits the encrypted files to a Time Source Provider along with the

client's Public Key. The associated attributes of the files, sizes, cryptographic signatures, etc, as well as the cryptographic signatures of both the Public and Private Keys, (also referred to as key fingerprints) are then encrypted first with the Private Key of the Client and then the Public Key of the Time Source Provider.

5 The Time Source Provider then decrypts the message with its Private Key (preferably unique to the client). The result is then decrypted with the Client's Public Key, verifying that it was the client that had sent an encrypted package. The accuracy of the associated attributes of the files are also verified. The Time Source Provider uses the files and attributes list and current time to create a time

10 map. This time map will use error correcting codes on one or more copies and one or more representations of time, as well as a transformation of the file attributes including sizes and cryptographic signature(s) together with the encryption key signatures provided by the client to scatter both the time representations and the file attributes, and signatures into a file of digital noise.

15 The result is then encrypted with a session key that is unavailable to the client. The client's original message and the generated time map, the cryptographic signature of the time map, and the cryptographic signature of the key used to encrypt the time map are encrypted with the Time Source Provider's Private key.

This encrypted message is then provided back to the client. The client

20 in turn decrypts the incoming message and verifies the signature of the time map for authenticity as having come from the designated Time Source Provider. The client then archives the files verifying sizes and signatures along with the file list including signatures, time and the time map. The client is then free to distribute the unencrypted files.

25 If the files themselves cannot be provided to the Time Source Provider for cryptographic signature verification due to perceived sensitivity, size, or other reasons, then the file attributes, together with both the cryptographic signature of the file and, a cryptographic signature of the file after encryption can be used. The cryptographic signature and the size of the encryption key used to encrypt the

30 file must also be supplied. These additional attributes would then also be

embedded in the time map. Existence of these attributes would indicate that the signatures were not verified. Additional strength can be added by adding file attributes in the form of cryptographic signatures of additional iterations of encryption with the same or different keys.

5 Additional benefits and advantages of the present invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by the practice of this invention. The advantages of this invention, as described herein, may be realized and obtained by means particularly pointed out and distinctly claimed in the appended claims, taken in
10 conjunction with the detailed specification.

DETAILED DESCRIPTION OF THE SPECIFICATION

15 The present invention provides a method for securing the chronological integrity of archived electronic documents or files as a means for certifying originality and ownership.

20 The present invention requires that there be a Time Source Provider, which is a separate entity (different from the client) providing a verifiable time stamp. Both the Time Source Provider and the Client require the ability to generate/acquire public and private key pairs. They will also exchange the Public Keys used in a secure fashion. There necessarily entails an exchange between the client and a Time Source Provider as will become more evident herein. The client and the Time Source Provider each have their own Public Key and Private Keys.

25 It should be understood that various alternative embodiments of the present invention are envisioned herein. Such variations involve differing degrees of strength of service provided by a Time Source Provider.

30 Generally, the client has one or more files which the client desires to be authenticated as having originated by the client prior to archiving. The client utilizes the methodology of the present invention prior to archiving the selected

files so that, in the future, should an instance arise wherein the client is called upon or otherwise has to authenticate the date and originality of a particular file, the archived version can be recalled and compared for authenticity. With the method of the present invention, authenticity can be assured at a subsequent 5 date.

The present method involves the client first generating or otherwise acquiring a Public and a Private Key pair. Preferably, the key pair is associated with an organization/corporate unit, or individual. A commercial or internal public key infrastructures can be used. The client shares their Public Key with the Time 10 Source Provider. The Time Source Provider similarly generates or acquires a Public and Private Key pair for use in transactions with the client, and shares the Public Key with the client.

The client then generates a list of files to be archived along with the files' respective file sizes and cryptographic signatures. The files are then 15 encrypted utilizing the client's Public Key. The cryptographic signatures are generated for the encrypted files, and the cryptographic signature of the Public Key used to encrypt the files is generated. Some clients might not want to reveal file names for security reasons, so optionally, the client could use a filename lookup table. The signature of that lookup table would need to be included in the 20 exchange of encrypted data between the client and the Time Source Provider. The client then encrypts the encrypted files and associated data first with their Private Key and then with the Time Source Provider's Public Key and transmits the encrypted files and data to a Time Source. This initiates the transaction. It is important to note that the medium of transport between the Time Source Provider 25 and the client can be an internet service, or a dial-up connection, or some other protocol agreed to by the parties. The Time Source Provider then decrypts the message first with the Time Source Provider's Private Key and then with the client's Public Key. The Time Source Provider verifies any signature of the client and the accuracy of the size and cryptographic signature attributes of the included 30 files. If the client has not included the encrypted files, then the data provided by

the client of signatures of the files after one or more iterations through encryption and the encryption key signatures are verified for format only. The Time Source Provider uses the files and attributes list and current time to create a time map.

The Time Map is a Session Key encrypted map of the time of recording 5 of the client's file information together with the actual information preferably scattered according to a function determined by the number of files, their sizes, their signatures and the current time. Preferably the time would be multiply represented and error correction codes applied. Also recorded in the time map is the time source, last synchronization to clock, location of the clock, last calibration 10 of the clock, and the last time that the encryption key(s) for data exchange were updated. The session key used to encrypt the time map is never shared with the client but is itself encrypted, and transmitted to a secured storage location along with the time map itself. The storage location preferably would not allow the information to be online in a network connected fashion for any length of time. 15 The information from the list would be selected to place the bits representing an absolute or relative time (or both) for a number of copies of the time (more than 1 for reasons of error detection and correction). Also embedded in the time map would be the list of files, file sizes, signatures, and any signatures of encrypted files. Also injected therein would be a fairly high volume (e.g. > 70%) of digital 20 noise.

Session Key exchange between the Time Source Provider and the client is known in cryptography texts such as the one by Bruce Schneier, Applied Cryptography 2 Ed. Session keys are usually symmetric keys such as DES because they are often much faster than Public Key/Private Key cryptography. 25 The session keys can be any encryption algorithm. Session Keys can also be used between client and Time Source Provider if additional security is required for the encryption of data file and attribute during transmission.

The client's original message and the generated time map are encrypted with the Time Source Provider's Private Key. Time map and session 30 key signatures are returned to the client. Client has responsibility for archiving

files, time map and the associated encryption key(s). The client in turn decrypts the incoming message and verifies the signature of the time map for authenticity as having come from the designated Time Source Provider. The client then archives the files verifying sizes and signatures along with the file list including 5 signatures, time and the time map. The client is then free to then distribute the unencrypted files.

In the event of request for legal verification of authenticity and/or the time of archival of files, the client would only have to produce the archived file and any encryption keys used by the client. The Time Source Provider would provide 10 evidence by retrieving the time map and the Session Key, regenerating the time map, from the components provided by the client, and encrypting it with the time map session key. The originality of the time and time map is then readily verified by comparing the regenerated time map to the time map in the possession of both the client and the Time Source Provider.

15 The Public Keys, the Session Keys, and the encrypted time map could be exchanged in X.509 or other format certificates known in the arts. Digital certificates add to the complexity of compromise, especially for "man in the middle" attacks where an interloper poses to be the client to the supplier, and the supplier to the client. Because encryption keys can be copied if inadequately 20 protected, adding a multi-factor authentication, such as a token or GPS would also add to the complexity of compromise. If a multi-factor authentication scheme such as SecurIDTM, CryptocardTM, or another system is used in conjunction with the exchange, it would also add to the security.

In the event wherein the timestamp is challenged, in the instance where 25 a claim is made that the files are newer than the timestamp, the timestamp was inaccurate, or someone other than the timestamping authority provided the timestamp, the client could show that the time map associated with one or more specific files could not have been deciphered, changed, nor reproduced by the client. If the timemap had been deciphered and substituted by the client, the 30 client would have also had to compromise the stores of the session keys and the

signature of the time map which are independently verifiable in the archives of the Time Source Provider. In addition, the time map reflects the time and the size and secure hash of the files in the scattering of time having been generated by the Time Source Provider during that particular timestamping session. The time map 5 could only have been accurately regenerated from files of the same sizes and secure hashes and only at the exact times listed in the time map. In order to make this event even more unlikely the client's encryption key fingerprint would also preferably be embedded in the time map generated by the Time Source Provider.

10 In the event that Company "A" is working on something that Company "B" is also working on and Company A wants to make sure that Company B does not complete the work first and perhaps gain market share, Company A might try to intercept Company B's files on their way to be time stamped at the Time Source Provider (provided that this information was known to Company A). This would 15 require Company A breaking the encryption that Company B uses with any given set of files and breaking that encryption and the time map as well. The methodology of the present invention thereby makes it even all the more difficult for industrial type espionage to have any likelihood of success.

20 In the instance of a "man in the middle" attack, where someone positions themselves to pretend to be the Time Source Provider, several alternatives could additionally be employed. For example, the keys exchanged between the client and the Time Source Provider could be embedded in any number of digital certificates thereby allowing for secure future checks from an independent Certificate Authority. In addition, the keys could be exchanged "out 25 of band", i.e. not over the network or internet. And for a slightly more secure method, one could use the public key encryption to negotiate one or more Session Keys to be used just for individual time stamping transactions.

30 Additionally, a "clear channel" transaction should take place on a periodic basis initiated by the client side which the time source would decrypt, and recognize the pattern, verifying that transmissions from the client weren't being

blocked. In the "clear channel" transaction, the time until the next "clear channel" and the pattern could be exchanged. This "clear channel" transaction could be encrypted using the same customer number keys used in normal transactions, so as not to alert an interceptor or some other entity desiring to disrupt 5 communication therebetween. Not receiving a "clear channel" by either party would trigger an alarm or warning of some kind at the Time Source Provider's end. The "clear channel" exchange could also embed an NTP transaction (the network time protocol) which would be a value added for the client as it could verify its internal time with the highly reliable time used by the Time Source Provider. The 10 Time Source Provider could also record the drift of client's internal clocks.

The Time Source Provider could also be setup so as to never be in a position to handle any unencrypted client files. Additionally, the integrity of the time acquisition software, and the time map generation software could be verified by a third party. Non-repudiation (digital signature) products exist such as 15 Approvit - Silanis Technology, which focus on document management and an approval. The Approvit package can detect alteration, but has no means of securing the timestamp (using the PC's own clock). Similarly, common digital signatures are not configured to prevent the acquisition of a timestamp followed by the generation of a file to match the file attributes.

20 In summary, what is presented is a novel method of securing the integrity of files prior to archiving such that the files' origin and authenticity can be subsequently and readily verified. The method of the present invention involves the steps wherein the client first generates or otherwise acquires a Public and a Private Key pair. Preferably, the key pair is associated with an 25 organization/corporate unit, or individual. If the key pair is reserved for archiving then the risk of exposure and compromising is decreased. Commercial or private key infrastructures can be leveraged in this acquisition, but are not required. The client then generates a list of files to be archived along with the files' respective file sizes and cryptographic signatures. The files data are then encrypted utilizing the 30 client's Public Key. The client transmits the encrypted files to a Time Source

Provider along with the client's Public Key. The associated attributes of the files, sizes, cryptographic signatures, etc, as well as the cryptographic signatures of both the public and private keys, (also referred to as key fingerprints) are then encrypted first with the Private Key of the Client and then the Public Key of the
5 Time Source Provider. The Time Source Provider then decrypts the message with its Private Key (preferably unique to the client). The result is then decrypted with the Client's Public Key, verifying that it was the client that had sent an encrypted package. The accuracy of the associated attributes of the files are also verified. The Time Source Provider uses the files and attributes list and current
10 time to create a time map. This time map will use error correcting codes on one or more copies and one or more representations of time, as well as a transformation of the file attributes (including sizes and cryptographic signature(s)) together with the encryption key signatures provided by the client to scatter both
15 the time representations and the file attributes, and signatures into a file of digital noise. The result is then encrypted with a session key that is unavailable to the client. The client's original message and the generated time map, the cryptographic signature of the time map, and the cryptographic signature of the key used to encrypt the time map are encrypted with the Time Source Provider's Private Key. This encrypted message is then provided back to the client. The
20 client in turn decrypts the incoming message and verifies the signature of the time map for authenticity as having come from the designated Time Source Provider. The client then archives the files verifying sizes and signatures along with the file list including signatures, time and the time map. The client is then free to distribute the unencrypted files.

25 With the above-described detailed description of the preferred embodiment (and the alternative embodiment) of the present invention and the above-described variations thereto, one skilled in the art of computer architecture and programming will readily find their specific implementation in accordance herewith.

This invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The above-described embodiments are to be considered in all respects only as illustrative and not restrictive in scope. The scope of the invention is, therefore, indicated by the 5 appended claims rather than by the above-detailed description. Therefore, all changes which come within the meaning and range of equivalency of the claims are to be considered embraced within their scope.

What is desired to be secured by United States Letters Patent is:

10

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
22310
22311
22312
22313
22314
22315
22316
22317
22318
22319
22320
22321
22322
22323
22324
22325
22326
22327
22328
22329
22330
22331
22332
22333
22334
22335
22336
22337
22338
22339
22340
22341
22342
22343
22344
22345
22346
22347
22348
22349
22350
22351
22352
22353
22354
22355
22356
22357
22358
22359
22360
22361
22362
22363
22364
22365
22366
22367
22368
22369
22370
22371
22372
22373
22374
22375
22376
22377
22378
22379
22380
22381
22382
22383
22384
22385
22386
22387
22388
22389
22390
22391
22392
22393
22394
22395
22396
22397
22398
22399
223100
223101
223102
223103
223104
223105
223106
223107
223108
223109
223110
223111
223112
223113
223114
223115
223116
223117
223118
223119
223120
223121
223122
223123
223124
223125
223126
223127
223128
223129
223130
223131
223132
223133
223134
223135
223136
223137
223138
223139
223140
223141
223142
223143
223144
223145
223146
223147
223148
223149
223150
223151
223152
223153
223154
223155
223156
223157
223158
223159
223160
223161
223162
223163
223164
223165
223166
223167
223168
223169
223170
223171
223172
223173
223174
223175
223176
223177
223178
223179
223180
223181
223182
223183
223184
223185
223186
223187
223188
223189
223190
223191
223192
223193
223194
223195
223196
223197
223198
223199
223200
223201
223202
223203
223204
223205
223206
223207
223208
223209
223210
223211
223212
223213
223214
223215
223216
223217
223218
223219
223220
223221
223222
223223
223224
223225
223226
223227
223228
223229
223230
223231
223232
223233
223234
223235
223236
223237
223238
223239
223240
223241
223242
223243
223244
223245
223246
223247
223248
223249
223250
223251
223252
223253
223254
223255
223256
223257
223258
223259
223260
223261
223262
223263
223264
223265
223266
223267
223268
223269
223270
223271
223272
223273
223274
223275
223276
223277
223278
223279
223280
223281
223282
223283
223284
223285
223286
223287
223288
223289
223290
223291
223292
223293
223294
223295
223296
223297
223298
223299
2232100
2232101
2232102
2232103
2232104
2232105
2232106
2232107
2232108
2232109
2232110
2232111
2232112
2232113
2232114
2232115
2232116
2232117
2232118
2232119
2232120
2232121
2232122
2232123
2232124
2232125
2232126
2232127
2232128
2232129
2232130
2232131
2232132
2232133
2232134
2232135
2232136
2232137
2232138
2232139
2232140
2232141
2232142
2232143
2232144
2232145
2232146
2232147
2232148
2232149
2232150
2232151
2232152
2232153
2232154
2232155
2232156
2232157
2232158
2232159
2232160
2232161
2232162
2232163
2232164
2232165
2232166
2232167
2232168
2232169
2232170
2232171
2232172
2232173
2232174
2232175
2232176
2232177
2232178
2232179
2232180
2232181
2232182
2232183
2232184
2232185
2232186
2232187
2232188
2232189
2232190
2232191
2232192
2232193
2232194
2232195
2232196
2232197
2232198
2232199
2232200
2232201
2232202
2232203
2232204
2232205
2232206
2232207
2232208
2232209
2232210
2232211
2232212
2232213
2232214
2232215
2232216
2232217
2232218
2232219
2232220
2232221
2232222
2232223
2232224
2232225
2232226
2232227
2232228
2232229
22322210
22322211
22322212
22322213
22322214
22322215
22322216
22322217
22322218
22322219
22322220
22322221
22322222
22322223
22322224
22322225
22322226
22322227
22322228
22322229
223222210
223222211
223222212
223222213
223222214
223222215
223222216
223222217
223222218
223222219
223222220
223222221
223222222
223222223
223222224
223222225
223222226
223222227
223222228
223222229
2232222210
2232222211
2232222212
2232222213
2232222214
2232222215
2232222216
2232222217
2232222218
2232222219
2232222220
2232222221
2232222222
2232222223
2232222224
2232222225
2232222226
2232222227
2232222228
2232222229
22322222210
22322222211
22322222212
22322222213
22322222214
22322222215
22322222216
22322222217
22322222218
22322222219
22322222220
22322222221
22322222222
22322222223
22322222224
22322222225
22322222226
22322222227
22322222228
22322222229
223222222210
223222222211
223222222212
223222222213
223222222214
223222222215
223222222216
223222222217
223222222218
223222222219
223222222220
223222222221
223222222222
223222222223
223222222224
223222222225
223222222226
223222222227
223222222228
223222222229
2232222222210
2232222222211
2232222222212
2232222222213
2232222222214
2232222222215
2232222222216
2232222222217
2232222222218
2232222222219
2232222222220
2232222222221
2232222222222
2232222222223
2232222222224
2232222222225
2232222222226
2232222222227
2232222222228
2232222222229
22322222222210
22322222222211
22322222222212
22322222222213
22322222222214
22322222222215
22322222222216
22322222222217
22322222222218
22322222222219
22322222222220
22322222222221
22322222222222
22322222222223
22322222222224
22322222222225
22322222222226
22322222222227
22322222222228
22322222222229
223222222222210
223222222222211
223222222222212
223222222222213
223222222222214
223222222222215
223222222222216
223222222222217
223222222222218
223222222222219
223222222222220
223222222222221
223222222222222
223222222222223
223222222222224
223222222222225
223222222222226
223222222222227
223222222222228
223222222222229
2232222222222210
2232222222222211
2232222222222212
2232222222222213
2232222222222214
2232222222222215
2232222222222216
2232222222222217
2232222222222218
2232222222222219
2232222222222220
2232222222222221
2232222222222222
2232222222222223
2232222222222224
2232222222222225
2232222222222226
2232222222222227
2232222222222228
2232222222222229
22322222222222210
22322222222222211
22322222222222212
22322222222222213
22322222222222214
22322222222222215
22322222222222216
22322222222222217
22322222222222218
22322222222222219
22322222222222220
22322222222222221
22322222222222222
22322222222222223
22322222222222224
22322222222222225
22322222222222226
22322222222222227
22322222222222228
22322222222222229
223222222222222210
223222222222222211
223222222222222212
223222222222222213
223222222222222214
223222222222222215
223222222222222216
223222222222222217
223222222222222218
223222222222222219
223222222222222220
223222222222222221
223222222222222222
223222222222222223
223222222222222224
223222222222222225
223222222222222226
223222222222222227
223222222222222228
223222222222222229
2232222222222222210
2232222222222222211
2232222222222222212
2232222222222222213
2232222222222222214
2232222222222222215
2232222222222222216
2232222222222222217
2232222222222222218
2232222222222222219
2232222222222222220
2232222222222222221
2232222222222222222
2232222222222222223
2232222222222222224
2232222222222222225
2232222222222222226
2232222222222222227
2232222222222222228
2232222222222222229
22322222222222222210
22322222222222222211
22322222222222222212
22322222222222222213
22322222222222222214
22322222222222222215
22322222222222222216
22322222222222222217
22322222222222222218
22322222222222222219
22322222222222222220
22322222222222222221
22322222222222222222
22322222222222222223
22322222222222222224
22322222222222222225
22322222222222222226
22322222222222222227
22322222222222222228
22322222222222222229
223222222222222222210
223222222222222222211
223222222222222222212
223222222222222222213
223222222222222222214
223222222222222222215
223222222222222222216
223222222222222222217
223222222222222222218
223222222222222222219
223222222222222222220
223222222222222222221
223222222222222222222
223222222222222222223
223222222222222222224
223222222222222222225
223222222222222222226
223222222222222222227
223222222222222222228
223222222222222222229
2232222222222222222210
2232222222222222222211
2232222222222222222212
2232222222222222222213
2232222222222222222214
2232222222222222222215
2232222222222222222216
2232222222222222222217
2232222222222222222218
2232222222222222222219
2232222222222222222220
2232222222222222222221
2232222222222222222222
2232222222222222222223
2232222222222222222224
2232222222222222222225
2232222222222222222226
2232222222222222222227
2232222222222222222228
2232222222222222222229
22322222222222222222210
22322222222222222222211
22322222222222222222212
22322222222222222222213
22322222222222222222214
22322222222222222222215
22322222222222222222216
22322222222222222222217
22322222222222222222218
22322222222222222222219
22322222222222222222220
22322222222222222222221
22322222222222222222222
22322222222222222222223
22322222222222222222224
22322222222222222222225
22322222222222222222226
22322222222222222222227
22322222222222222222228
22322222222222222222229
223222222222222222222210
223222222222222222222211
223222222222222222222212
223222222222222222222213
223222222222222222222214
223222222222222222222215
223222222222222222222216
223222222222222222222217
223222222222222222222218
223222222222222222222219
223222222222222222222220
223222222222222222222221
223222222222222222222222
223222222222222222222223
223222222222222222222224
223222222222222222222225
223222222222222222222226
223222222222222222222227
223222222222222222222228
223222222222222222222229
2232222222222222222222210
2232222222222222222222211
2232222222222222222222212
2232222222222222222222213
2232222222222222222222214
2232222222222222222222215
2232222222222222222222216
2232222222222222222222217
2232222222222222222222218
2232222222222222222222219
2232222222222222222222220
2232222222222222222222221
2232222222222222222222222
2232222222222222222222223
2232222222222222222222224
2232222222222222222222225
2232222222222222222222226